



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,155	08/01/2006	Makoto Kagaya	MIY.001.0045.PC	4105
58789 7590 03/02/2010 NDQ&M WATCHSTONE LLP 1300 EYE STREET, NW SUITE 1000 WEST TOWER WASHINGTON, DC 20005				
EXAMINER				
ZIA, SYED				
ART UNIT		PAPER NUMBER		
2431				
MAIL DATE		DELIVERY MODE		
03/02/2010		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/588,155

**Applicant(s)**

KAGAYA ET AL.

**Examiner**

SYED ZIA

**Art Unit**

2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 01 August 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SF/ICE)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

This office action is in response to application filed August 1, 2006. Claims 1-16 are pending.

#### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(c) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-16 are rejected under 35 U.S.C. 102(c) as being anticipated by Murakami et al. (U.S. Patent No.: 6,996,724)

1. Regarding Claim 1, Murakami teach and describe a secret information management system for managing a secret information of a user, comprising: a data division unit configured to divide the secret information into a plurality of divided data by using a secret sharing scheme, such that the secret information can be recovered from a prescribed number of the divided data; a divided data storing unit configured to store a part of the plurality of divided data into a terminal of the user as user's divided data, and a rest of the plurality of divided data into one or more of deposit servers; a data re-division unit configured to generate a plurality of re-divided data different from the plurality of divided data obtained by the data division unit, from a combination

of the prescribed number of the divided data among the divided data stored in the deposit servers by using the secret sharing scheme; and a re-divided data storing unit configured to store a part of the plurality of re-divided data into the terminal as newly generated user's divided data and a rest of the plurality of re-divided data into the deposit servers as newly generated divided data (Fig.2-4, and col.6 line 26 to col.8 line 60).

2. Regarding Claim 15, Murakami teach and describe a secret information management method for managing a secret information of a user, comprising the steps of: dividing the secret information into a plurality of divided data by using a secret sharing scheme, such that the secret information can be recovered from a prescribed number of the divided data; storing a part of the plurality of divided data into a terminal of the user as user's divided data, and a rest of the plurality of divided data into one or more of deposit servers; generating a plurality of re-divided data different from the plurality of divided data obtained by the dividing step, from a combination of the prescribed number of the divided data among the divided data stored in the deposit servers by using the secret sharing scheme; and storing a part of the plurality of re-divided data into the terminal as newly generated user's divided data and a rest of the plurality of re-divided data into the deposit servers as newly generated divided data (Fig.2-4, and col.6 line 26 to col.8 line 60).

3. Regarding Claim 16, Murakami teach and describe a computer program product for causing a computer to function as a secret information management system for managing a secret information of a user, the computer program product comprising: a first computer program code

for causing the computer to divide the secret information into a plurality of divided data by using a secret sharing scheme, such that the secret information can be recovered from a prescribed number of the divided data; a second computer program code for causing the computer to store a part of the plurality of divided data into a terminal of the user as user's divided data, and a rest of the plurality of divided data into one or more of deposit servers; a third computer program code for causing the computer to generate a plurality of re-divided data different from the plurality of divided data obtained by the first computer program code, from a combination of the prescribed number of the divided data among the divided data stored in the deposit servers by using the secret sharing scheme; and a fourth computer program code for causing the computer to store a part of the plurality of re-divided data into the terminal as newly generated user's divided data and a rest of the plurality of re-divided data into the deposit servers as newly generated divided data (Fig.2-4, and col.6 line 26 to col.8 line 60).

4. Claims 1-14 are rejected applied as above rejecting Claim 1. Furthermore, Murakami teach and describe a method

As per Claim 2, further comprising: a data recovery unit configured to acquire the user's divided data, and recover the secret information from a combination of the prescribed number of the divided data among the user's divided data and the divided data stored in the deposit servers by using the secret sharing scheme, at a time of utilizing the secret information (Fig.2-4, and col.6 line 26 to col.8 line 60)

As per Claim 3, further comprising: a utilization log memory unit configured to store a fact that the secret information is utilized as a utilization log information, at a time of utilizing the secret information (Fig.2-4, and col.6 line 26 to col.8 line 60).

As per Claim 4, further comprising: a divided data transmission unit configured to transmit a combination of as many of the divided data stored in the deposit servers as the prescribed number minus a number of the divided data maintained by the user, to the terminal, at a time of recovering the secret information (Fig.2-4, and col.6 line 26 to col.8 line 60).

As per Claim 5, further comprising: a transmission unit configured to transmit the part of the divided data to be stored into the terminal, to the terminal through a communication network (Fig.2-4, and col.6 line 26 to col.8 line 60).

As per Claim 6, further comprising: a reception unit configured to receive the secret information from the terminal through a communication network (Fig.2-4, and col.6 line 26 to col.8 line 60).

As per Claim 7, the data division unit and the data re-division unit use the secret sharing scheme which is a data division method for dividing the secret information into the divided data in a desired number of division according to a desired processing unit bit length, in which the divided data in the desired number of division are generated by generating a plurality of original partial data by partitioning the secret information in units of the processing unit bit length, generating a plurality of random number partial data of the processing unit bit length from a random number in a length shorter than or equal to a bit length of the secret information, in correspondence to respective ones of the plurality of original partial data, and generating each divided partial data in the processing unit bit length that constitutes each divided data by

calculating exclusive OR of the original partial data and the random number partial data, and the re-divided data in the desired number of division are generated by generating a plurality of new random number partial data of the processing unit bit length from a newly generated random number, and generating the re-divided partial data in the processing unit bit length by calculating exclusive OR of the divided partial data and the new random number partial data(Fig.2-5, and col.6 line 26 to col.8 line 60,and co.11 line 6 to line 47).

As per Claim 8, wherein the data re-division unit generates the re-divided data by calculating exclusive OR of the divided partial data that constitute each divided data contained in a combination of the prescribed number of the divided data(Fig.2-4, and col.6 line 26 to col.8 line 60).

As per Claim 9, wherein the data division unit and the data re-division unit use the secret sharing scheme which generates each re-divided partial data that constitutes each re-divided data by calculating exclusive OR of each divided partial data and the new random number partial data corresponding to the random number partial data used in generating each divided partial data (Fig.2-5, and col.6 line 26 to col.8 line 60 and col.11 line 6 to line 47).

As per Claim 10, wherein the data division unit and the data re-division unit use the secret sharing scheme in which old random number partial data are deleted from each re-divided partial data that constitutes each re-divided data by calculating exclusive OR of each re-divided partial data and the old random number partial data used in generating each divided partial data corresponding to each re-divided partial data (Fig.2-4, and col.6 line 26 to col.8 line 60).

As per Claim 11, wherein the data division unit and the data re-division unit use the secret sharing scheme in which the desired number of division is  $n=3$ , the divided partial data

$D(i,j)$  ( $i=1$  to  $3$ ,  $j=1$  to  $2$ ) that constitute each divided data are modified by interchanging  $D(1,j+1)$  and  $D(2,j+1)$  (Fig.2-4, and col.6 line 26 to col.8 line 60).

As per Claim 12, the data division unit and the data re-division unit use the secret sharing scheme in which the desired number of division is  $n$ ,  $n \geq 4$ , the divided partial data  $D(i,j)$  ( $i=1$  to  $n$ ,  $j=1$  to  $n-1$ ) that constitute each divided data are modified by setting a new value of  $D(1,j)$  to be exclusive OR of  $D(1,j)$  and  $D(n,j)$ , and then rotating  $D(1,j)$ ,  $D(2,j)$ ,  $\dots$   $D((n-1),j)$  (Fig.2-4, and col.6 line 26 to col.8 line 60).

As per Claim 13, the data division unit and the data re-division unit use the secret sharing scheme in which  $D(1,j)$ ,  $D(2,j)$ ,  $\dots$   $D((n-1),j)$  are rotated for  $(i-1)$  times (Fig.2-4, and col.6 line 26 to col.8 line 60).

As per Claim 14, the data re-division unit generates the plurality of re-divided data from a combination of the prescribed number of the divided data among the divided data stored in the deposit servers and the user's divided data stored in the terminal, upon receiving the user's divided data from the terminal, and the re-divided data storing unit stores a part of the plurality of re-divided data into another terminal of another user as another user's divided data and a rest of the plurality of re-divided data into the deposit servers as new divided data, at a time of transferring an access right for the secret information from the user to the another user (Fig.2-5, and col.6 line 26 to col.8 line 60 and col.11 line 6 to line 47).

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz  
February 26, 2009  
/Syed Zia/  
Primary Examiner, Art Unit 2431